

UNITED NATIONS



NATIONS UNIES

OFFICE OF INTERNAL OVERSIGHT SERVICES

INTERNAL AUDIT DIVISION

Ref. No.

AO-4/02

7-1:31 (1542/02)

23 October 2002

Assignment No. AF2002/21/2

To: Mr. Paul Aghadjanian, Chief Administrative Officer, a.i.
UNOHCI

From:

Jayanti Prasad, Chief Resident Auditor

UNOHCI

Internal Audit Division, OIOS

Subject: **Audit of Information Technology and Communications in UNOHCI**

The recommendations set out below are submitted for your consideration. Please comment on them and, where appropriate, specify the corrective action taken or provide a planned implementation schedule. When commenting please refer to the Assignment No. listed above and to the recommendation number in parenthesis in order to facilitate monitoring of its status (timely response, acceptance, implementation). Please reply by 23 November 2002.

Audit Observations and Recommendations

1. Communications and Information Technology are critical to the activities of UNOHCI. The 'Communications and Information Technology Section' (CITS) in UNOHCI, Baghdad has overall responsibility to provide voice and data communication needs of UNOHCI and UN Agencies in Iraq. Within UNOHCI, it has the responsibility to plan, install, maintain and manage all communication equipment and Information Technology (IT) hardware and software.
2. The expenditure on communications in UNOHCI for the years 2000 and 2001 was \$1.06 million, and constituted 12% of the Non-Personnel costs. In the year 2002, of

the local procurement in UNOHCI of over \$5 million, 24% (\$1.2 million) was spent on Communications and 11% (\$ 0.56 million) was spent on EDP.

3. The 'Information and Communications Technology Board' (ICTB) has been established by Secretary General's Bulletin (ST/SGB/2001/5) with the overall goal to ensure that the information and communication technology needs of the department are identified and met. The bulletin enjoins the offices away from the headquarters to form local information and communication technology groups on the same pattern.

4. There is no separate IT policy in UNOHCI. The general policies of UNHQ and DPKO, and orders issued by ICTB from time to time guide the efforts in this area. We are of the opinion that, since EDP does not only effect but many a times defines the way business is done, there is a need for inputs from a cross-section of IT users, in the planning process due to specific local needs.

We recommend:

UNOHCI form an 'Information and Communication Technology' group with objectives as cited in the SGB, with representation from different sections of UNOHCI. This would ensure that information technology and communication initiatives of UNOHCI are aligned with the needs of the organization (AF02/21/2/101)

5. The Chief, Communications and Information Technology Section (CCITS) is the head of section in UNOHCI at Baghdad. The Deputy, CCITS in Erbil has the operational responsibility for the three northern governorates. In the present setup, both Communications and Information Technology are under a single operational head, who are essentially communications experts. Though there is a post of IT Supervisor (Deputy Chief EDP) in Baghdad, it has not been staffed for more than 2 years.

We recommend that UNOHCI:

- (i) Practice in mission to have one section each for Communications and EDP (AF02/21/2/102); and
- (ii) Fill the vacancy of IT supervisor in Baghdad (AF02/21/2/103).

Job Descriptions

6. Segregation of duties assumes a very important role in the Information Technology set up for the added reason that audit trails cannot be easily established and accountability cannot be easily assigned. Thus, it is imperative that critical responsibilities are defined. In order to examine the existence and efficacy of this internal control, we asked for the job descriptions of the staff in the CITS to examine them for appropriate segregation of duties.

7. Our discussions brought out that appropriate segregation in roles did not exist. In Erbil, all EDP staff had 'super user' status, which dilutes accountability.

We recommend that UNOHCI:

- (i) Review the access privileges of the EDP staff and ensure that privileged access is granted only to a few on a need basis (AF02/21/2/104); and

Staff Deployment

8. The Communication and Information Technology section is responsible for providing telephone and data communication (Lotus Notes) to all the UN agencies in Iraq. The number of personnel for the UN agencies and hence the clientele is larger in North. Approximately 64% of the international staff are in North and only 36% in Baghdad.

9. Within the mission areas CITS also provides radio communication. In Baghdad the radio communication network is limited to the city. In the North, the radio

network exists in each of the governorates as well as additional UNGCI team bases locations at Diana and Zakho. The radio control rooms are manned by security/UNGCI in various locations. Staff members are provided with hand held radio sets and the vehicles are equipped with radios for movement tracking and control. Repeaters have been installed at various sites by CITS to inter-link all the locations in North. In order to assess whether the staff deployment is in proportion to the workload, we collected the number of CITS staff at all locations and compared with the number of international staff (all agencies). The results are depicted in the table below:

Location	Client Size (Number of International Staff)		Number of Communications & IT Staff	
	Number	Percentage	Number	Percentage
Baghdad	310	36.34	31	62
Erbil	353	41.4	12	24
Duhok	78	9.1	4	8
Suleymaniah	112	13.1	3	6
Total	853	100	50	100

10. Therefore, the staffing at various locations has little correlation with the clientele which has been taken as a measure of the workload. The statistical correlation between the client size and service staff was only 0.71. While approximately 62 % of CITS staff was servicing 36% of Clients in Baghdad, only 38% of CITS staff was left to service 64% of clients in North, despite the fact that the geographical area in the North was larger and the terrain more difficult.

11. The number of staff in the Communication and IT section at the various locations, in terms of international and local staff, is given in the following table:

Location	Number of International Staff	Number of Local Staff	Total
Baghdad	12	19	31
Erbil	6	6	12
Duhok	1	3	4
Suleymaniah	0	3	3

12. From the above we can see that most of the CITS staff is local. In Suleymaniah there was no international staff. Since, CITS has access to sensitive data and information we are of the opinion that in all locations international staff should man the key positions.

We recommend that UNOHCI:

- (i) Conduct a comprehensive review of workload for "Communications and Information Technology" and re-deploy staff as per the workload to correct the skewed deployment of staff in Baghdad when compared to North. (AF02/21/2/105); and
- (ii) Identify the key job functions in all locations and ensure that there is an international staff to handle the key responsibilities (AF02/21/2/106).

Password Management

13. IT systems in UNOHCI process and store a wide variety of information. Information residing on a system that is accessed by many users, can also create problems. A significant concern is ensuring that users have access to information that they need, but do not have access to sensitive information.

14. Logical access controls are protection mechanisms that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them. Passwords are probably the most common way of protecting information on IT systems in that they are the most frequently used means for users to be identified and

authenticated on the system. Thus, they are often the first line of protection afforded in an IT system.

15. The primary advantage of password-based logical access control is that it is provided by a large variety of PC applications and thus often does not have to be implemented as a new/separate feature on an operating system. The drawbacks of this approach center on the difficulty for users to manage even moderate numbers of passwords. The security of a password-based system is significantly diminished when users are not educated and perform actions like writing down/storing their passwords.

16. In UNOHCI no password policy exists except that occasionally a mail is sent from the IT section asking users to change passwords.

We recommend that UNOHCI:

- (i) Maintain and enforce password history¹ of five (AF02/21/2/107);
- (ii) Have a maximum password age² of two months (AF02/21/2/108);
- (iii) Set minimum password length to six characters (AF02/21/2/109);
- (iv) Enforce a mix of alphabets and numeric in passwords (AF02/21/2/110); and
- (v) Disable reversible encryption storage of passwords (AF02/21/2/111).

17. Furthermore, account lock out policy, by way of which invalid attempts to access IT systems are tracked, is an important tool for preventing and detecting unauthorized access to the system. We found that no such policy was in place in UNOCHI.

¹ Number of previous passwords remembered by the system

² Time period after which password automatically expires.

We recommend that UNOHCI:

- (i) Establish an account lockout threshold³ to five attempts (AF02/21/2/112);
- (ii) Set account lockout duration⁴ to 5 minutes (AF02/21/2/113);
- (iii) Reset account lockout counter after first successful logon (AF02/21/2/114); and
- (iv) On successful logon notify the user of the last logon and failed logon attempts. (AF02/21/2/115).

Internet Access

18. E-mail and web access is provided to all the staff members through the LAN. Shareable computers have been provided for web and e-mail access to those staff members who do not have a PC allocated to them. Having guidelines for the usage of these facilities is a necessary control. Since complete monitoring of web access may not be practical, there is a need for user being made aware of the organization's policies and guidelines on the issue. There are also certain undesirable sites on the Internet, which the UN may want to actively block out for its staff members. We observed that in UNOHCI there is a filtering software "Super Scout" which was being used to filter undesirable sites during the working hours only.

³ Specifies the number of invalid attempts before the account is locked out.

⁴ The duration for which account is locked out.

We recommend that UNOHCI:

- (i) Incorporate a welcome screen message on logging on to the network, which informs users about UN policy on use of the Internet (AF02/21/2/116); and
- (ii) Have screening software to block out undesirable sites from the Internet to the users at all times (AF02/21/2/117).

Email management

19. The guidelines for the use of e-mail system in the United Nations are set forth in Information Circular ST/IC/2002/70. These guidelines state that e-mail services are for the exchange of business communication and information and is not meant to be used as a filing system or storage device.

20. The guideline lays down a message retention policy for messages in Inbox, Sent Folder, User Folder, Draft Folder, Stationary Folder, Trash Folder, Calendar items and To-do list items. Furthermore, in order to mitigate the risk of overload to the mail server there is a policy of deleting all e-mail messages having an attachment of more than 2 MB.

21. We found that no such message retention policy was in place in UNOHCI. Though the users are asked to restrict their mail file size to 30 MB and advised to archive the mail locally, this was not being enforced. In UNOHCI Erbil out of 87 registered e-mail users, as many as 53 had mail files of 24 MB or more, on a particular day. This reveals that non-enforcement of the policy was leading to extra load being put on the server.

22. Furthermore, we found that the all the address books were accessible to all the e mail users. This allowed access to group emails for all staff members and there was a possibility of spamming. Since the Notes e-mail facility is used for official purpose, we feel that group-mailing option needs to be restricted.

We recommend that UNOHCI:

- (i) Establish a message retention policy on the lines of UNHQ and enforce it through the system (AF02/21/2/118);
- (ii) Restrict access to e-mail to those who need it (AF02/21/2/119); and
- (iii) Restrict access to group mail addresses to authorized staff members on a need basis (AF02/21/2/120).

Physical Security

23. Physical security of the IT assets used to be the only access control mechanism in the past. Even now it remains one of the most important access control. The critical assets need to be kept secure since a threat to them translates into much larger damage. The servers are the most critical aspects of the system. Their physical as well as logical security is critical for the organization.

24. We found that server rooms had adequate physical security and were kept locked. However, no logs were being maintained for the access to the server room. In absence of such logs it would not be possible to trace back any damage to the system to an individual.

We recommend UNOHCI maintain a log for the physical access to the server room. The log should include the name of the staff member, date/time of access and the reasons for such access. (AF02/21/2/121).

Voice Communication and billing

25. CITS provides the backbone for communication link between all UN agencies in Iraq and the outside world through UNLB. Earth satellite stations have been established in all locations. The link between these locations and UNLB is used for all voice and data communication.

26. The earth satellite stations at all the locations link to UN Logistics Base, Brindisi and thus become a part of the UN Global network. Bandwidth is acquired for each location and UNLB. Subsequently, this bandwidth is apportioned between data and voice channels. This is the sole link between the locations and the outside world. The installation and maintenance of all kind of communication equipment from satellite stations to telephone instruments is the responsibility of CITS.

27. The voice communication services provided by UNOHCI are made available to staff members for personal use on a payment basis as per the UN policy. The rates for calls to various destinations are laid down and revised from time to time. It is the responsibility of the executive officer to recover the cost of personal calls.

28. For UNOHCI staff members a T-pin is assigned to all the staff members for international dialing facility. A bill is generated every month for all the staff members and given to them for certifying these as official or personal calls. The personal calls of a staff member are recovered from next month's MSA. For the UN agencies the T-pins are shared with their staff members. Bills are therefore generated agency wise and sent to the agencies for recovering the cost of personal calls.

29. In the present system as we can see that there is a delay of at least a month between the personal calls being made and those actually recovered, due to the fact the billing cycle is also calendar month like MSA payment.

30. In UNOHCI T-Pin assignment, we saw from the bill that in certain cases the T-pins were assigned by name to the staff member while in other cases the T-Pins were assigned to the staff member by designation. There seemed to be no policy governing such assignments. We are of the opinion that the accountability is better when the T-Pins are assigned by name so that the individual is held accountable for it.

31. We found that though the agencies were given monthly telephone bills, no mechanism was in place to ensure that cost of personal calls was actually recovered. Since cross billing between the agencies has been discontinued, the agencies are not required to pay UNOHCI for the official calls any more. Our discussions with the

Administrative Officer, UNDP brought out that there was no foolproof method of identifying the personal calls from the consolidated T-pin bills received by them. In practice the personal calls were being identified by circulating the consolidated bill to all staff members and asking them to identify their calls. It is obvious that such a system inherently treats all the calls as official unless certified otherwise. In such a system, if for any reason a personal call cannot be identified, costs have to be borne by the UN.

32. We examined UNDP's telephone bill for a selected month. We found that from the UNDP switch board there were calls over \$3,538 in August 2002. It was not possible to ascertain what amount of this was personal. However, a perusal of the destinations indicated that many of these were personal calls. However, UNDP had only been able to identify and collect about \$8,000 in the whole year. This was indicative of the fact that the controls required to bring to account the UN money was weak.

33. We found that there were apparent mistakes in the telephone bills of UNOHCI in Dohuk and Suleymaniah. Certain calls were not linked to any extension and the "calling party" was shown as "UNDEFINED" in the bill for the month of July '02 for Dohuk. In Suleymaniah several calls were shown from an extension number "21000" which apparently does not exist. Furthermore, in the Suleymaniah telephone bill the name of the "calling party" was not mentioned against any extension number.

34. When these irregularities were pointed out to the Deputy CITS, he replied that these mistakes were corrected manually in Baghdad. Furthermore, we found that though the telephone billing system was much bigger in North (covering three governorates and all agency personnel), the billing system in North was still centralized in Baghdad. There was no staff member for setting up the billing system specifically and presently a staff member from Radio room and another has been diverted for setting up the billing in North.

We recommend that UNOHCI:

- (i) Change the billing cycle for the phone calls from 20th of the preceding month to 20th of the current month and the cost of personal calls

be recovered from the MSA due at the end of the current month (AF02/21/2/122);

(ii) Assign T-Pins by name rather than designation in order to ensure better control and accountability (AF02/21/2/123);

(iii) Obtain a certificate from the heads of the UN agencies every month that the personal calls have actually been billed and recovered (AF02/21/2/124);

(iv) Establish a system, in consultation with the UN agencies, to ensure that systems are in place for individual accountability for the calls from the Agency T-Pins (AF02/21/2/125);

(v) Explore the possibility of assigning unique T-pins individually to international staff of Agencies instead of T-pins to the Agency as a whole. This should be possible with the recent up-gradation of the exchanges in UNOHCI (AF02/21/2/126);

(vi) Establish a proper telephone billing system in the North, so that there is no need for manual intervention in rectifying telephone bills (AF02/21/2/127); and

(vii) Establish a billing unit with a supervisor in UNOHCI, North (AF02/21/2/128).

35. UNOHCI has a LAN installed in each of the locations, which are interconnected in a wide area network. The objectives of networking is to have increased efficiency by sharing of data and IT resources.

36. However, we found that very little data was being shared on the network and e-mail connectivity was the only tangible benefit of networking. In fact the users are not allowed to share their disk data directly and the shared drive for the purposes of sharing did not have much data to share. All the users have their own printers and

other IT equipment. This in our view, was sub-optimal use of the investment in the network resources. Specially in the view of existence of a facility like LOTUS Notes

We recommend that UNOHCI:

- (i) Develop applications and institute measures for better utilization of network. Often used forms like MOP, F-10, etc. should be kept on the shared drive only. (AF02/21/2/129); and
- (ii) Determine the feasibility to develop applications for automation of submission and processing of various forms may be explored. (AF02/21/2/130)

Policy on cordless telephone sets in North

37. In the North, a few staff members have been provided with "Senao" cordless sets linked to their land lines. The range of these handheld cordless sets is 1-2 kilometers. These phone sets ensure that the staff members are connected at all times and can be contacted, while away from their offices.

38. However, we found that no formal policy existed for allocating these cordless phone sets. They were being authorized and issued on an ad-hoc basis. Since North Iraq is in the Phase IV of security and also there is no local telephone system existing, we believe that it is necessary to provide all international staff with telephone connectivity at all times. These sets cost only about \$200-\$300.

We recommend UNOHCI to:

- (i) Issue "Senao" cordless phones to all the international staff members in North. (AF02/21/2/131); and
- (ii) Formulate a policy for issuing "Senao" phones to few key local staff in North, taking into consideration the level of the staff and the need for him to be contacted in emergencies etc. (AF02/21/2/132).

39. All the four locations in Iraq have a voice link, a data link and an asynchronous voice/data link through UNLB. The bandwidth leased for each of the locations is as follows:

	Baghdad	Erbil	Suleymaniah	Dohuk
Asymmetric (Voice/Data)	256/192	256/128	192/128	192/128
Voice	193	16	193	193
Data	193	32	193	193 ⁵

- All bandwidth in Kbps

40. We studied the traffic analysis for each of these links. Details were collected for the yearly average utilization of the data links. The results are summarized in the following table:

	Baghdad				Erbil				Suleymaniah				Dohuk			
	In		Out		In		Out		In		Out		In		Out	
	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg
Asym	6.8	2.5	14.9	7.9	34	13.3	88	70.3	2.7	1	6.8	2.6	1.3	0.9	7.1	2
Voice	.5	0.3	1.5	0.4	13	7.2	14.3	7.8	0.8	0.4	0.7	0.4	0.6	0.3	0.6	0.3
Data	8.3	2.2	14.4	7.4	28.9	8.4	81.3	58.3	2.3	0.8	5.8	2.1	0.9	0.4	6.5	1.6 ⁶

⁵ All bandwidth in kbps

⁶ The figures above are percentage figures of utilization out of the available bandwidth.

41. From the foregoing table it is apparent that proper planning has not been done for the bandwidth allocation at the various locations. The percentage utilization is very low in Suleymaniah and Dohuk and very high in Erbil.

We recommend that UNOHCI conduct a review of actual bandwidth requirements at various locations and change the contracted bandwidth in line with actual requirements (AF02/21/2/133).

42. We thank UNOHCI for the cooperation extended to the Auditors during the conduct of this audit.

Cc:

Mr. Ramiro Lopes Da Silva, Humanitarian Coordinator, UNOHCI

Mr. Tesfaye Maru, Dy. Humanitarian Coordinator, UNOHCI

Mr. Michael Brown, OIC (Administration), UNOHCI, North